Light-Weighted DNA based Hybrid Cryptographic Mechanism against Chosen Cipher Text Attacks

E Suresh Babu\textsuperscript{a}, C Nagaraju\textsuperscript{b}, MHM Krishna Prasad\textsuperscript{c}

\textsuperscript{a}JNTUK Kakinada, KLEF, K L University, AP, India.
\textsuperscript{b}YSR Engineering College of YV University, AP, India.
\textsuperscript{c}College of Engineering, JNTUK, AP, India.

DNA Cryptography is a new cryptographic paradigm from hastily growing bio molecular computation, as its computational power will determine next generation computing. As technology is growing much faster, data protection is getting more important and it is necessary to design the unbreakable encryption technology to protect the information. In this paper, we proposed a biotic DNA based secret key cryptographic mechanism, seeing as DNA computing had made great strides in ultra-compact information storage, vast parallelism, and exceptional energy efficiency. This Biotic Pseudo DNA cryptography method is based upon the genetic information on biological systems. This method makes use of splicing system to improve security, random multiple key sequence to increase the degree of diffusion and confusion, which makes resulting cipher texts difficult to decipher and makes to realize a perfect secrecy system. Moreover, we also modelled Hybrid DNA cryptosystem that make use of proposed work by assembling DNA based public key cryptography for effective storage of public key as well as double blinded encryption scheme for a given message. The formal and experimental analysis not only shows that this method is powerful against brute force attack and chosen cipher text attacks, but also it is very efficient in storage, computation as well as transmission.

**Keywords**: Brute Force Attack and Chosen Cipher Text Attack, DNA based Symmetric Cryptography.

1. INTRODUCTION

DNA Computing is a Bio-Molecular Computation (BMC), which makes use of biological methods for performing massively parallel computation. As Power of the parallel processing is increasing day to day, modern cryptosystems can be easily cryptanalyzed by the cryptanalyst, the world is looking for new ways of information and network security in order to safeguard the data as it carries. The purpose of using cryptography in the areas of bio-molecular computation to bring up a promising technology for providing of unbreakable algorithms. DNA Cryptography is a new cryptographic paradigm from hastily growing bio-molecular computation, in which its computational power will determine next generation computing. As internet technology is growing much faster, which permits the users to access the intellectual property that is being transferred over the internet can be easily acquired and is vulnerable to many security attacks such as Worm Hole attack, IP Spoofing, Black Hole Attack and Man in the middle attack [1][2][3] etc.,.

Subsequently, securing all the information passed through networked computers is primarily more important for any application or system. Already a great heap of effort had been put on the cryptologys, As a result, various security mechanisms have been designed such as DES, RSA, ECC, DSA etc., to achieve very high level of security. However, these mechanisms require complex factorization of large prime numbers and the elliptic curve problem, for which still a lot of investigation is required to find
proposed algorithm needs the 264, 310, 410, 575 chosen cipher texts to find the message without key for different key size.

As shown in the Figure 4. The length of cipher texts is proportional to that of the corresponding plaintexts lengths with varying key length. However, this method requires less storage space than that of the plaintext, thus, it is more efficient in the storage capacity. Another reflection is that, the size of the random key length increase as the size of the plaintext increase, which greatly reduces size of the key length. Moreover, key as well cipher text can be transmitted much faster through the secure channel and public channel respectively. Therefore, the method is also more efficient in terms of storage and transmission. As shown in the above Figure 5. The adversary requires more than 65% of chosen cipher texts for the corresponding plaintexts to recover 78% of the random key length. Hence, it requires more chosen cipher text to retrieve the key. The figure also shows that different tests are performed to experiment the robustness of this proposed method. Therefore, it is more efficient and effective method.

The above Figure 6 indicates, for the same plaintext length, it generates different cipher text, namely cipher text-1 and cipher text-2 with different random key. Thus, this method satisfies the Message Indistinguishability (MI) because the probability of guessing these two cipher text is more than half of the random probability of guessing the right message.

The above Figure 7 shows that the adversary requires more chosen cipher text for a given plaintext, which takes more than half of the time to retrieve the key. Therefore, PPT algorithm satisfies Message Indistinguishability (MI), according to the definition.

11. CONCLUSIONS

In this paper, we addressed a biotic DNA based secret key cryptographic mechanism, which is based upon the genetic information of biological system. Moreover, this cryptographic prototype is motivated from bio-molecular computation, which is rapidly growing field that has made great strides of ultra-compact information storage, vast parallelism, and exceptional energy efficiency. Over the last two decades, Internet technology is growing much faster, which permits the users to access the intellectual property that is being transferred over the internet can be easily acquired and is vulnerable to many security attacks. Hence, network security is looking for unbreakable encryption technology to protect the data. This motivated us to propose biotic pseudo DNA cryptography method, which makes use of splicing system to improve security and random multiple key sequence to increase the degree of diffusion and confusion that makes resulting cipher texts difficult to decipher and to realize a secure system. Furthermore, Moreover, we also modelled Hybrid DNA cryptosystem that make use of proposed work by assembling DNA based public key cryptography for effective storage of public key as well as double blinded encryption scheme for a given message. The formal and experimental analysis not only shows that, this method is powerful against chosen cipher text attacks, but also very effective and efficient in storage, computation as well as transmission; To conclude, DNA cryptography is an new emerge area and extremely guaranteeing field, where research is possible in incredible development and improvement.

REFERENCES


22. Boris Shimanovsky, Jessica Feng and Miodrag Potkonjak. Hiding Data in DNA, Dept. of Computer Science, University of California, Los Angeles.


29. Miki Hirabayashi, Akio Nishikawa, Fumiaki Tanaka, Masami Hagiya, Hironori Kojima and Kazuhiro Oiwa. Analysis on Secure and Effective Applications of a DNA-Based Cryptosystem, In Proceedings of Sixth International Con-


41. L H N C for Biomedical Communications, Handbook on Genetic Cells and DNA. USA: National Library of Medicine, National Institutes of Health, Department of Health and Human Services, 2010.


E Suresh Babu received his BTech Degree in Computer Science Engineering from RGM College of Engineering, Nandyal, MTech Degree in Computer Science from V T University Belgaum and pursuing Ph.D in Computer Science and Engineering from J N T U Kakinada. Currently, he is working as an Associate Professor in the Department of CSE in K L University Vijayawada. He has 12 years of teaching experience. He has published 12 research papers in various International Journal and 10 research papers in various National and International Conferences. He has attended 32 seminars and workshops. His areas of interests are Wireless Networks, Network Security and MANETs, Cognitive Radio Networks, Software Radio Networks.

C Naga Raju is currently working as Associate Professor and Head of the Department of Computer Science and Engineering at YSR Engineering College of Yogivemana University, Poddatur, Kadapa District and Andhra Pradesh, India. He received his BTech Degree in Computer Science from J N T University, Anantapur and MTech Degree in Computer Science from J N T University Hyderabad and Ph.D in Digital Image Processing from J N T University Hyderabad. He has got 18 years of teaching experience. He received research excellence award, teaching excellence award and Rayalaseema vidhyaratna award for his credit. He wrote text book on and Data structures. He has six Ph.D scholars. He has published fifty three research papers in various National and International Journals and about thirty research papers in various National and International Conferences. He has attended twenty seminars and workshops. He is member of various professional societies like IEEE, ISTE and CSI.
Munaga H M Krishna Prasad is currently an Associate Professor of the Department of Computer Science and Engineering, University College of Engineering, Kakinada (Autonomous), JNTUK, Andhra Pradesh. He did his BE from Osmania University, Hyderabad, MTech and Ph.D Computer Science and Engineering from JNTU, Hyderabad. He successfully completed a two year MIUR fellowship at University of Udine, Udine, Italy. He has about 50 research papers in various International Journals and Conferences and attended many national and international conferences in India and abroad. He is a member of Association for Computing Machinery (ACM), ISTE and IAENG (Germany) is an active member of the board of reviewers in various International Journals and Conferences. His research interests include Data Mining, Big Data Analytics and High Performance Computing.